

TD

WWW.SMIA2.COM

Algèbre I

S 1

TD intégrale
2012/2013

MR BOUHAMZA

SERIE 1

Exercice 1.

Soit E et F deux ensembles. Montrer que : $E \cap F = E \cup F \Leftrightarrow E = F$.

Exercice 2.

Soit E, F et G trois ensembles. Montrer que :

1) $E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$

2) $E \cap (F \cup G) = (E \cap F) \cup (E \cap G)$.

Exercice 3

Soit E un ensemble, A et B deux parties de E . Montrer que :

1) $\mathcal{C}_E^{A \cap B} = \mathcal{C}_E^A \cup \mathcal{C}_E^B$.

2) $\mathcal{C}_E^{A \cup B} = \mathcal{C}_E^A \cap \mathcal{C}_E^B$.

Exercice 4

Soit E, F et G trois ensembles tels que : $E \cap F = F \cap G$ et $E \cup F = E \cup G$.

Montrer que : $F = G$.

Exercice 5

Soit E un ensemble, A et B deux parties de E . Montrer que : $\mathcal{C}_E^{A-B} = B \cup \mathcal{C}_E^A$.

Exercice 6

Soit $E = \{2u / u \in \mathbb{Z}\}$ et $F = \{3v / v \in \mathbb{Z}\}$. Déterminer $E \cap F$.

Exercice 7

Soit E et F deux ensembles. Montrer que : $(E - F = F - E) \Leftrightarrow (E = F)$

Exercice 8

Soit $(E_n)_{n \in \mathbb{N}}$ une suite de parties de $\mathbb{N}$ et soit $E = \{n \in \mathbb{N} / n \notin E_n\}$

Montrer que pour tout $n \in \mathbb{N}$, on a : $E \neq E_n$.





Serie ① : Ex 1:

Soit E et F deux ensembles. Mq $E \cap F = E \cup F \Leftrightarrow E = F$

$$E = F \Leftrightarrow (E \subset F \text{ et } F \subset E)$$

$$E = F \Leftrightarrow E \subset F \text{ et } F \subset E$$

$$\Rightarrow E \subset E \cup F$$

$$\text{et } F \subset E \cup F$$

$$\Rightarrow E \cap F \subset E \cup F$$

$$\text{Mq } E \cup F \subset E \cap F$$

Solution:

1) Supposons que $E \cup F = E \cap F$ et montrons que $E = F$

i. Soit $x \in E$ on a $x \in E \cup F$ car $E \subset E \cup F$

$$\text{or comme } E \cup F = E \cap F$$

$$\text{on a } x \in E \cap F$$

il en résulte que $x \in F$ ce qui montre que $E \subset F$

ii. Preuve montrer que $F \subset E$ on procede de la même façon

Donc si $E \cap F = E \cup F$, on a $E = F$

2. Supposons que $E = F$ et montrons que $E \cap F = E \cup F$

$$\text{Comme } E = F \text{ on a } E \cap F = E \text{ et } E \cup F = E$$

$$\text{D'où } E \cap F = E \cup F$$

Remarque:

si $E \neq F$ on a $E \cap F \neq E \cup F$.

Ex 2:

Soit E , F et G trois ensembles. Mq

$$D) E \cup (F \cap G) = (E \cup F) \cap (E \cup G)$$

$$\begin{aligned} x \in E \text{ ou } (x \in F \text{ et } x \in G) &\Rightarrow (x \in E \text{ ou } x \in F) \text{ et } (x \in E \text{ ou } x \in G) \\ &\Rightarrow (E \cup F) \cap (E \cup G) \end{aligned}$$

Solution:

methode ①

$$\text{On a } F \cap G \subset E \cup F \text{ car } F \cap G \subset F$$

on a $F \cap G \subset G \subset E \cup G$
d'où $F \cap G \subset (E \cup F) \cap (E \cup G)$ (1)

on a $E \subset E \cup F$ et $E \subset E \cup G$

donc $E \subset (E \cup F) \cap (E \cup G)$ (2)

D'après (1) et (2) on a $E \cup (F \cap G) \subset (E \cup F) \cap (E \cup G)$.
méthode (2) :

Pour montrer que

$$E \cup (F \cap G) \subset (E \cup F) \cap (E \cup G)$$

soit $x \in E \cup (F \cap G)$

On a $x \in E$ ou $x \in F \cap G$

* Si $x \in E$ alors comme $E \subset E \cup F$ et $E \subset E \cup G$

on a $x \in E \cup F$ et $x \in E \cup G$

D'où $x \in (E \cup F) \cap (E \cup G)$

** si $x \in F \cap G$

alors $x \in F$ et $x \in G$ et comme

$F \subset E \cup F$ et $G \subset E \cup G$

on a $x \in E \cup F$ et $x \in E \cup G$

D'où $x \in (E \cup F) \cap (E \cup G)$

$$(E \cup F) \cap (E \cup G) \subset E \cup (F \cap G)$$

soit $x \in (E \cup F) \cap (E \cup G)$

$x \in (E \cup F)$ et $x \in (E \cup G)$

si $x \in E$

Alors $x \in F$ et $x \in G$

d'où $x \in (F \cap G)$

Donc $x \in E \cup (F \cap G)$

$$(E \cup F) \cap (E \cup G) \subset E \cup (F \cap G)$$



Ex 3:

soit E un ensemble A et B deux parties de E

$$\text{D) } Mq: C_E^{A \cap B} = C_E^A \cup C_E^B$$

soit $x \in C_E^{A \cap B} \Rightarrow x \notin A \cap B$
 $\Rightarrow x \in C_E^A \text{ ou } x \in C_E^B$
 $\Rightarrow x \in C_E^A \cup C_E^B$
 $\Rightarrow C_E^{A \cap B} \subset C_E^A \cup C_E^B$

$$Mq: C_E^A \cup C_E^B \subset C_E^{A \cap B}$$

soit $x \in (C_E^A \cup C_E^B)$

$$\text{On a: } x \in C_E^A \text{ ou } x \in C_E^B$$

$$\text{d'où } x \notin A \text{ ou } x \notin B$$

$$\text{on en déduit que } x \notin A \cap B$$

$$\text{donc } x \in C_E^{A \cap B}$$

$$\text{d'où } C_E^A \cup C_E^B \subset C_E^{A \cap B}$$

ce qui montre que $F \subset G$

De la même façon on montre que $G \subset F$

Ex 5:

soit E, A et B deux parties de E .

Mq:

$$C_E^{A-B} = B \cup C_E^A$$

$$Mq: C_E^{A-B} \subset B \cup C_E^A$$

$$\text{soit } x \in C_E^{A-B}$$

$$\text{on a } x \notin A - B$$

$$\text{Alors } x \notin A \text{ ou } x \in B$$

$$\text{d'où } x \in C_E^A \text{ ou } x \in B$$

$$\text{par suite: } x \in B \cup C_E^A$$

$$\text{tg: } B \cup C_E^A \subset C_E^{A-B}$$

$$\text{soit } x \in B \cup C_E^A$$

$$\text{On a } x \in B \text{ ou } x \in C_E^A$$

$$\text{Alors } x \in B \text{ ou } x \notin A$$

$$\text{d'où } x \notin (A - B)$$

$$\text{par suite } x \in C_E^{A-B}$$

donc:

$$B \cup C_E^A \subset C_E^{A-B} \Rightarrow B \cup C_E^A = C_E^{A-B}$$

Ex 6:

$$\text{Soit } x \in E \cap F$$

$$\text{On a alors } x \in E \text{ et } x \in F$$

$$\text{Il existe donc } u \in \mathbb{Z}$$

$$\text{tel que } x = 2u.$$

$$\text{et il existe } v \in \mathbb{Z}$$

$$\text{tel que } x = 3v$$

$$\text{Ainsi on a } 2u = 3v$$

$$\text{On en déduit que 3 divise } 2u.$$

Ex 4:

soit E, F , et G trois ensembles tg:

$$E \cap F = E \cap G \text{ et } E \cup F = E \cup G$$

$$Mq: F = G$$

$$Mq: F \subset G$$

$$\text{soit } x \in F$$

$$\text{comme } F \subset E \cup F$$

$$\text{or comme } E \cup F = E \cup G$$

$$\text{on a } x \in E \cup G$$

$$\text{si } x \notin E \text{ alors } x \in G$$

$$\text{si } x \in E \text{ alors } x \in E \cap F \text{ et par suite}$$

$$x \in E \cap G$$

$$\text{d'où } x \in G.$$

comme $3 \nmid 2 = 1$

d'après le théorème de Gauss

$3 \mid u$. Il existe donc $k \in \mathbb{Z}$

$$\text{tq } u = 3k$$

$$\text{D'où } x = 2u = 2 \cdot 3k = 6k$$

Il en résulte que

$$E \cap \mathbb{Z} \subset \{6k / k \in \mathbb{Z}\}$$

Réciproquement,

$$\text{soit } x \in \{6k / k \in \mathbb{Z}\}$$

$$\text{on a } x = 6k$$

$$= 2 \cdot (3k) \in E$$

$$= 3 \cdot (2k) \in F$$

Donc $x \in E \cap F$ et par suite

$$\{6k / k \in \mathbb{Z}\} \subset E \cap F$$

ce qui montre que

$$E \cap F = \{6k / k \in \mathbb{Z}\}$$

$$E \cap \mathbb{Z}$$

$$\text{or } (E - F) = (F - E)$$

$$\text{donc } E = F.$$

Ex 8 :

soit $(E_n)_{n \in \mathbb{N}}$ une suite de parties de $\mathbb{N}$ et soit $E = \{n \in \mathbb{N} / n \notin E_n\}$.

En raisonnant par l'absurde
supposons qu'il existe $n \in \mathbb{N}$

$$\text{tq } E = E_n$$

Deux cas sont possibles

$$\text{1er cas : } n \in E_n$$

$$\text{alors } n \notin E$$

contradiction avec le fait

$$\text{que } E = E_n$$

$$\text{2ème cas : } n \notin E_n$$

$$\text{alors } n \in E$$

contradiction avec le fait

$$\text{que } E = E_n$$

$$\text{D'où } E \neq E_n.$$

Exo 7 :

soit E et F deux ensembles

$$\text{M.q. } (E - F) = (F - E) \Leftrightarrow E = F$$

$$\text{M.q. } (E - F) = (F - E) \Rightarrow E = F$$

$$\text{On a } E = (E - F) \cup (E \cap F)$$

$$\text{et } F = (F - E) \cup (E \cap F)$$

SMIA2

SERIE 2

Exercice 1.2

Soit E, F deux ensembles et f une application de E vers F . Montrer que :

$$f \text{ est bijective} \Leftrightarrow \forall X \in P(E) : f(\mathcal{C}_E^X) = \mathcal{C}_F^{f(X)}.$$

Exercice 2.2

Soit E, F deux ensembles et f une application de E vers F telle que :

pour tout $(X, Y) \in P(E) \times P(E)$ on a : $f(X \cap Y) = f(X) \cap f(Y)$

Montrer que f n'est pas injective.

Exercice 3.2

Soit E, F deux ensembles et f une application de E vers F . On considère l'application :

$$g : P(E) \longrightarrow P(F)$$

$$X \longrightarrow f(X)$$

1) Montrer que g est bijective.

2) Déterminer g^{-1} .

Exercice 4.2

On considère l'application $E : \mathbb{R} \longrightarrow \mathbb{Z}$
$$x \longrightarrow E(x)$$

où $E(x)$ est l'élément de $\mathbb{Z}$ défini par : $E(x) \leq x < E(x)+1$.

1) Montrer que E n'est pas injective.

2) Montrer que E est surjective.

3) Soit $n \in \mathbb{Z}$. Déterminer $E^{-1}(n)$.

4) Déterminer $E(\mathbb{Z})$.

5) Soit $A = \{-\sqrt{6}, -\sqrt{5}, -\sqrt{3}, \sqrt{3}, \sqrt{5}, \sqrt{6}\}$. Déterminer $E(A)$.



Exercice 5.2

Soit E un ensemble, A et B deux parties de E et $f: P(E) \longrightarrow P(E) \times P(E)$

non vide

$$X \longrightarrow (A \cup X, B \cup X)$$

Montrer que f n'est pas surjective.

Exercice 6.2

Soit E, F, G trois ensembles, f une application de E vers F , g une application de F vers G et $h = g \circ f$.

Montrer que :

- 1) si g est injective et h est surjective alors f est surjective.
- 2) si f est surjective et h est injective alors g est injective.

Exercice 7.2

Soit E un ensemble, f, g et h trois applications de E vers F telles que : $g \circ f = f \circ h = e$ où désigne l'application de E vers E définie pour tout élément x de E par $e(x) = x$.

- 1) Montrer que f est bijective.
- 2) Montrer que $g = h$.
- 3) Montrer que $g = f^{-1}$.

NB: $f: E \longrightarrow F$
 f est dite surjective si : $\forall y \in F, \exists x \in E, y = f(x)$

→ Co Exercice 5.2 :

• Si $E = \emptyset$, on a $A = B = \emptyset$

$$P(E) = \{\emptyset\}$$

$$P(E) \times P(E) = \{(\emptyset, \emptyset)\}$$

Alors f est surjective



Ex 1:

$$f: E \rightarrow F$$

Montrer que

$$f \text{ bijective} \iff \forall x \in P(E): f(C_E^x) = C_F^{f(x)}$$

i - supposons f bijective et montrons que

$$\forall x \in P(E), f(C_E^x) = C_F^{f(x)}$$

soit $x \in P(E)$

$$f(C_E^x) \subset C_F^{f(x)}$$

* - Soit $x \in f(C_E^x)$ il existe alors $y \in C_E^x$ tel que $x = f(y)$ si $x \notin C_F^{f(x)}$, on aurait

$x \in f(x)$. Il existerait un élé z de X tel que $x = f(z)$

Ainsi on aurait $f(y) = f(z)$

et comme f est injective

on aurait $z = y$

contradiction avec

en fait que $y \in C_E^x$ et $z \in X$

Donc $x \in C_F^{f(x)}$

ce qui montre que $f(C_E^x) \subset C_F^{f(x)}$

** Réciproquement, soit $y \in C_F^{f(x)}$

soit $y \in C_F^{f(x)}$

comme f est surjective

il existe un élément x de E

tel que $y = f(x)$

si $x \in X$ on aurait $f(x) \in f(X)$

D'où $y \in f(X)$ ce qui

contradiquerait $y \in C_F^{f(x)}$

Donc $x \notin X$ c'est à dire

que $x \in C_E^x$

Il en résulte que

$$f(x) \in f(C_E^x)$$

D'où $y \in f(C_E^x)$

ce qui montre que

$$C_F^{f(x)} \subset f(C_E^x)$$

ii - supposons que $\forall x \in P(E)$

$$f(C_E^x) = C_F^{f(x)}$$

et montrons que f est bijective

* Montrons que f est injective

Pour cela, soit x et y deux

éléments de E tels que $f(x) = f(y)$

En raisonnant par l'absurde

supposons $x \neq y$

Il en résulte que $y \in C_E^{f(x)}$

et par suite $f(y) \in f(C_E^{f(x)})$

or d'après notre hypothèse

$$\text{on a } f(C_E^{f(x)}) = C_F^{f(f(x))} = C_F^{f(f(y))}$$

D'où $f(y) \in C_F^{f(f(x))}$

On en déduit que $f(y) \neq f(x)$

(p a)

Montrons que f est surjective

Pour cela, soit y un

élément de F

$$\text{On a: } f(C_E^E) = C_F^{f(E)}$$

$$f(\emptyset) = C_F^{f(\emptyset)}$$

$$\varnothing = \bigcup_F \mathcal{P}(E)$$

On en déduit que $f(E) = F$

Il en résulte que $y \in f(E)$

Il existe donc $x \in E$ tel

que $y = f(x)$

ce qui montre que f est surjective

Ex 2:

Soit E, F deux ensembles et f

une application E vers F

Montrer que

f est injective $\Leftrightarrow$

$\forall X, Y \in \mathcal{P}(E)$

On a $f(X \cap Y) = f(X) \cap f(Y)$

i. supposons f injective

et montrons que $\forall X, Y \in \mathcal{P}(E)$

On a $f(X \cap Y) = f(X) \cap f(Y)$

Soit X, Y deux éléments de $\mathcal{P}(E)$

* Montrons tout d'abord que

$$f(X \cap Y) \subset f(X) \cap f(Y)$$

soit $y \in f(X \cap Y)$

Il existe alors $x \in X \cap Y$

tel que $y = f(x)$

On a $x \in X$ et $x \in Y$

D'où $f(x) \in f(X)$ et $f(x) \in f(Y)$

$\Rightarrow f(x) \in f(X) \cap f(Y)$

Donc $y \in f(X) \cap f(Y)$

ce qui montre que

$$f(X \cap Y) \subset f(X) \cap f(Y)$$

* Montrons maintenant que

$$f(X) \cap f(Y) \subset f(X \cap Y)$$

soit $y \in f(X) \cap f(Y)$

on a $y \in f(X)$ et $y \in f(Y)$

Il existe donc $u \in X$ et $v \in Y$ tels que

$$y = f(u) \text{ et } y = f(v)$$

$$\text{D'où } f(u) = f(v)$$

Comme f est injective

$$\text{On a } u = v$$

ainsi $u \in X \cap Y$

$$\text{d'où } f(u) \in f(X \cap Y)$$

$$\text{càd } y \in f(X \cap Y)$$

ce qui montre que $f(X) \cap f(Y) \subset f(X \cap Y)$

ii. supposons que $\forall X, Y \in \mathcal{P}(E)$

$$f(X \cap Y) = f(X) \cap f(Y)$$

et montrons que f est injective

soit $x, x' \in E : f(x) = f(x')$

$$\text{On a } f(x) \in f(\{x\})$$

$$\text{et } f(x') \in f(\{x'\})$$

$$f(x) = f(x') \in f(\{x\}) \cap f(\{x'\})$$

si $x \neq x'$

$$\text{On a } \{x\} \cap \{x'\} = \varnothing$$

$$f(\{x\} \cap \{x'\}) = f(\varnothing) = \varnothing$$

et $f(x) \in \varnothing$ contradiction

Alors $x = x'$

Donc f est injective

Rappel:

$$f(A) = \{ f(x) / x \in A \} = \{ f(x) \} \text{ et } (f \circ g)(x) = \{ f(t) / t \in \{x\} \} = \{ f(t) / t = x \}$$

Ex 3:

Soit E, F deux ensembles et f une application bijective de E vers F .

$$g : P(E) \rightarrow P(F)$$

$$X \rightarrow f(X)$$

1) Montrer que g est bijective

2) Déterminer g^{-1}

D i. Montrons que f est bijective

Soit X et Y deux éléments de $P(E)$

tels que $g(X) = g(Y)$.

on a alors $f(X) = f(Y)$

Soit $x \in X$ on a $f(x) \in f(X)$

or $f(X) = f(Y)$

il en résulte que $f(x) \in f(Y)$

$f(x) \in f(Y)$ on en déduit qu'il

existe $y \in Y$ tel que $f(x) = f(y)$

comme f est bijective on $x = y$.

Ainsi on a $x \in Y$

ce qui montre que $X \subset Y$

De façon analogue

on montre que $Y \subset X$

N'ai $X = Y$

et par suite g est injective.

Ex 6:

$$E: \mathbb{R} \rightarrow \mathbb{Z}$$

$$x \rightarrow E(x)$$

où $E(x)$ est l'élément de $\mathbb{Z}$ défini

par $E(x) \leq x < E(x) + 1$

1) $M. g. E$ n'est pas injective

2) $M. g. E$ est surjective

3) Soit $n \in \mathbb{Z}$. Déterminer $E^{-1}(n)$

4) Déterminer $E(\mathbb{Z})$

5) Soit $A = \{-\sqrt{6}, -\sqrt{5}, -\sqrt{3}, \sqrt{3}, \sqrt{5}, \sqrt{6}\}$

Déterminer $E(A)$

solution:

1) E n'est pas injective $\Leftarrow \exists (x, x') \in \mathbb{R}^2 / x \neq x' / E(x) = E(x')$

$$\text{On a } (0, \frac{1}{2}) \in \mathbb{R}^2 \text{ tq } 0 \neq \frac{1}{2}$$

$$E(0) = E(\frac{1}{2}) = 0$$

N'ai E n'est pas injective.

2) $M. g. E$ est surjective

Soit $y \in \mathbb{Z}$ alors $E(y) = y$.

N'ai $\forall y \in \mathbb{Z} \exists x \in \mathbb{R} \text{ tq } E(x) = y$.
ce qui montre que E est surjective.

3) $E^{-1}(n) = \{x \in \mathbb{R} / E(x) = n\}$

$$E(x) = n \Leftrightarrow x \in [n, n+1[$$

$$\text{Donc } E^{-1}(n) = [n, n+1[$$

$$f: \begin{matrix} E \\ \cup \\ A \end{matrix} \rightarrow F$$

$$f(A) = \{ f(x) / x \in A \}$$

$$4) E(\mathbb{Z}) = \{ E(x) / x \in \mathbb{Z} \}$$

$$= \{ x / x \in \mathbb{Z} \}$$

$$= \mathbb{Z}$$

SMIA 2

Ex 5:

$$f: P(E) \rightarrow P(E) \times P(E)$$

$$X \rightarrow (A \cup X, B \cup X)$$

Montrons que f n'est pas surjective

En raisonnant par l'absurde.

Supposons f surjective

On en déduit qu'il existe

$X \in P(E)$ tel que

$$f(X) = (\emptyset, \emptyset)$$

$$\text{D'où } A \cup X = \emptyset \text{ et } B \cup X = \emptyset$$

$$\Rightarrow A = B = \emptyset$$

De même il existe $Y \in P(E)$ tq $f(Y) = (E, \emptyset)$

$$A \cup Y = E \text{ et } B \cup Y = \emptyset$$

$$\Rightarrow Y = E \text{ et } Y = \emptyset$$

$$\Rightarrow E = \emptyset \text{ contradiction}$$

avec le fait que $E \neq \emptyset$

Donc f n'est pas surjective.

Ex 6:

$$f: E \rightarrow F$$

$$g: F \rightarrow G$$

$$h: g \circ f: E \rightarrow G$$

i) Soit $y \in F$. Posons $z = g(y)$

comme h est surjective, il existe

$x \in E$ tel que $z = h(x)$

On en déduit que

$$z = g \circ f(x) = g[f(x)]$$

Ainsi que l'on a $g(y) = g[f(x)]$

Comme g est injective

$$\text{on a } y = f(x).$$

ce qui montre que f est surjective.

2) si f est surjective et h est injective alors g est injective

soit $y, y' \in F$ tq $g(y) = g(y')$

comme f est surjective alors

$$y = f(x) \text{ et } y' = f(x')$$

$$\Rightarrow g \circ f(x) = g \circ f(x')$$

$$\text{c'ad } h(x) = h(x')$$

et comme h est injective alors $x = x'$

$$\text{Donc } f(x) = f(x')$$

$$\text{d'où } y = y'$$

ce qui montre que g est injective.

Ex 7:

i) Montrons que f est injective

Pour cela soit x, x' deux éléments

de E tq $f(x) = f(x')$

On en déduit que

$$g(f(x)) = g(f(x'))$$

$$g \circ f(x) = g \circ f(x')$$

$$e(x) = e(x')$$

$$x = x'$$

ce qui montre que f est injective

ii. Montrons que f est surjective

Pour cela soit $y \in E$

Alors on a $f \circ h(y) = e(y) = y$

$$f(h(y)) = y.$$

$$\text{En posant } h(y) = x$$

$$\text{on a } f(x) = y$$

ce qui montre que f est surjective et par suite f est bijective.



SERIE 3

Exercice 1.3

On considère dans $\mathbb{R}$ la relation d'équivalence R définie pour tout $(x, y) \in \mathbb{R}^2$ par :

$$x R y \Leftrightarrow x^3 - 6x = y^3 - 6y.$$

Soit $a \in \mathbb{R}$. Déterminer la classe d'équivalence $\bar{a}$ de a modulo R .

Exercice 2.3

Soit E un ensemble non vide et A une partie non vide de E .

1) Soit $X \in P(A)$ et $Y \in P(E)$ tels que : $A \cup X = A \cup Y$. Montrer que $Y \in P(A)$.

2) Soit $X \in P(E)$ tel que : $A \cap X = \emptyset$ et soit $Y \in P(E)$ tel que : $A \cup X = A \cup Y$.

Montrer qu'il existe $B \in P(A)$ tel que $Y = X \cup B$.

3) Soit $X \in P(E)$ tel que : $A \cap X \neq \emptyset$ et soit $Y \in P(E)$ tels que : $A \cup X = A \cup Y$.

Montrer qu'il existe $B \in P(A)$ tel que $Y = B \cup C_X^{A \cap X}$.

4) On considère dans $P(E)$ la relation d'équivalence R définie par :

$$X R Y \Leftrightarrow X \cup A = Y \cup A.$$

Soit $X \in P(E)$. Déterminer la classe d'équivalence $\bar{X}$ de X modulo R .

Exercice 3.3

Soit E, F deux ensembles, R une relation d'équivalence dans E et S une relation d'équivalence dans F . On considère dans $E \times F$ la relation binaire T définie par :

$$(x, y) T (x', y') \Leftrightarrow (x R x' \text{ et } y S y')$$

1) Montrer que T est une relation d'équivalence dans $E \times F$.

2) Soit $(a, b) \in E \times F$. Déterminer la classe d'équivalence $\overline{(a, b)}$ de (a, b) modulo T .

3) On considère l'application $f : E \times F / T \rightarrow E / R \times F / S$
 $\overline{(a, b)} \rightarrow (\bar{a}, \bar{b})$

Montrer que f est bijective.

Exercice 4.3

Soit $E = \mathbb{Z} \times \mathbb{Z}^*$. On considère dans E la relation binaire R définie par :

$$(a, b) R (c, d) \Leftrightarrow ad = bc.$$

1) Montrer que R est une relation d'équivalence dans E .

2) Soit p et q deux éléments de $\mathbb{Z}$ premiers entre eux.

Montrer que la classe d'équivalence $\overline{(p, q)}$ de (p, q) modulo R est $\{(pn, qn) / n \in \mathbb{Z}^*\}$.

3) Soit $(a, b) \in E$ et $d = a \wedge b$. On pose $a = du$ et $b = dv$.

Montrer que $\overline{(a, b)} = \overline{(u, v)}$.

4) On considère l'application : $f : \mathbb{Z} \rightarrow E / R$
 $a \rightarrow \overline{(a, 1)}$

Montrer que f est injective.

Ex 1:

On considère dans $\mathbb{R}$ la relation

d'équivalence R définie par

$$x R y \Leftrightarrow x^3 - 6x = y^3 - 6y$$

Déterminer $\bar{a}$

$$\bar{a} = \{x \in \mathbb{R} / x R a\}$$

$$= \{x \in \mathbb{R} / x^3 - 6x = a^3 - 6a\}$$

$$= \{x \in \mathbb{R} / x^3 - 6x - a^3 + 6a = 0\}$$

$$= \{x \in \mathbb{R} / (x-a)(x^2 + ax + a^2 - 6) = 0\}$$

$$= \{x \in \mathbb{R} / x = a \text{ ou } x^2 + ax + a^2 - 6 = 0\}$$

Résolvons l'équation

$$x^2 + ax + a^2 - 6 = 0$$

$$\Delta = a^2 - 4(a^2 - 6)$$

$$= 3(8 - a^2)$$

$$\Delta = 0 \Leftrightarrow a = \pm 2\sqrt{2}$$

$$\text{si } a \in]-2\sqrt{2}, 2\sqrt{2}[$$

On a $\Delta < 0$

$$\text{si } a \in]-\infty, -2\sqrt{2}[\cup]2\sqrt{2}, +\infty[$$

On a $\Delta > 0$

$$\text{Donc si } a = \pm 2\sqrt{2}$$

l'équation admet une seule solution: $\pm \sqrt{2}$

si $a \in]-2\sqrt{2}, 2\sqrt{2}[$ l'équation admet 2 solutions

$$\text{si } a \in]-\infty, -2\sqrt{2}[\cup]2\sqrt{2}, +\infty[$$

l'équation n'admet pas de solution

$$-a - \frac{\sqrt{3(8-a^2)}}{2} \text{ et } -a + \frac{\sqrt{3(8-a^2)}}{2}$$

Conclusion:

$$\text{i si } a \in]-\infty, -2\sqrt{2}[\cup]2\sqrt{2}, +\infty[$$

$$\bar{a} = \{a\}$$

$$\text{ii si } a = -2\sqrt{2}$$

$$\bar{a} = \{-2\sqrt{2}, \sqrt{2}\}$$

$$\text{iii si } a = 2\sqrt{2}, \bar{a} = \{2\sqrt{2}, -\sqrt{2}\}$$

$$\text{iv si } a \in]-2\sqrt{2}, 2\sqrt{2}[$$

$$\bar{a} = \left\{a, \frac{-a - \sqrt{3(8-a^2)}}{2}, \frac{-a + \sqrt{3(8-a^2)}}{2}\right\}$$

Ex 2:

Soit E un ensemble non vide et A

une partie non vide de E

1. Soit $x \in P(A)$ et $y \in P(E)$

tel que $A \cup x = A \cup y$

Montrer que $y \in P(A)$

• Soit $x \subset y$. Alors comme

$$y \subset A \cup y$$

$$\text{On a } x \subset A \cup y$$

$$\text{et comme } A \cup y = A \cup x$$

$$\text{On a } x \subset A \cup x$$

$$\text{or } x \subset A \text{ d'où } A \cup x = A$$

et par suite $x \subset A$

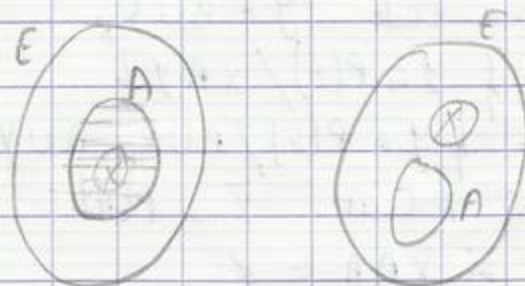
Ce qui montre que $y \in P(A)$

2) Soit $x \in P(E)$ et $A \cap x = \emptyset$ et

Soit $y \in P(E)$ tel que $A \cup x = A \cup y$

Montrons que

il existe $B \in P(A)$ / $y = x \cup B$



soit $x \in Y$ on a $x \notin A$ ou $x \in X$

Soit $B = \{x \in Y / x \notin X\}$

On a $B \subset A$ et $Y \subset B \cup X$

De même on a $B \cup X \subset Y$

D'où $Y = B \cup X$

3. Soit $X \in P(E)$ tel que

$A \cap X \neq \emptyset$ et $Y \in P(E)$

tel que $A \cup X = A \cup Y$

Montrons qu'il existe $B \in P(A)$

tel que

$$Y = B \cup C_x^{A \cap X}$$

• Soit $B = \{x \in Y / x \notin X \cup (A \cap X)\}$

Soit $x \in Y$ alors on a $x \in A$ ou $x \in X$

i. si $x \in X$ et $x \notin A$ alors $x \notin A \cap X$

$$\Rightarrow x \in C_x^{A \cap X}$$

ii. si $x \in A$ et $x \notin X$ alors $x \in B$

iii. si $x \in A \cap X$ alors $x \in B$

D'où $Y \subset B \cup C_x^{A \cap X}$

soit $x \in C_x^{A \cap X}$ alors $x \in X$ et $x \notin A$

$$\Rightarrow x \in Y$$

$$\Rightarrow C_x^{A \cap X} \subset Y$$

aussi $B \cup C_x^{A \cap X} \subset Y$

et par suite $Y = B \cup C_x^{A \cap X}$

4. $\bar{X} = \{Y \in P(E) / X \cap Y = \emptyset\}$

$$= \{Y \in P(E) / A \cup X = A \cup Y\}$$

i. si $X \subset A$ $\bar{X} = P(A)$

ii. si $X \cap A = \emptyset$

$$\bar{X} = \{X \cup B / B \in P(A)\}$$

iii. si $X \cap A \neq \emptyset$

$$\bar{X} = \{B \cup C_x^{A \cap X} / B \in P(A)\}$$

SMIA 2

Ex 3:

$$(x, y) T (x', y') \Leftrightarrow (x R x' \text{ et } y S y')$$

D) Montrons que T est une relation

d'équivalence dans $E \times F$

1) soit $(a, b) \in E \times F$

$$(\overline{a}, \overline{b}) = ?$$

$$2. (\overline{a}, \overline{b}) = \{ (x, y) \in E \times F / (a, b) T (x, y) \}$$

$$= \{ (x, y) \in E \times F / a R x \text{ et } b S y \}$$

$$= \{ (x, y) \in E \times F / x \in \overline{a} \text{ et } y \in \overline{b} \}$$

$$= \overline{a} \times \overline{b}$$

$$3. f: E \times F / T \longrightarrow E/R \times F/S$$

$$(\overline{a}, \overline{b}) \longmapsto (\overline{a}, \overline{b})$$

montrer que f est bijective:

i) Montrons que f est injective

Soit (a, b) et (c, d)

deux éléments de $E \times F$ tels que

$$f(\overline{a}, \overline{b}) = f(\overline{c}, \overline{d})$$

On a

$$(\overline{a}, \overline{b}) = (\overline{c}, \overline{d})$$

$$\overline{a} = \overline{c} \text{ et } \overline{b} = \overline{d}$$

On en déduit que

$a R c$ et $b S d$

$$\text{D'où } (a, b) T (c, d)$$

$$\text{D'où } \text{Donc } (\overline{a}, \overline{b}) = (\overline{c}, \overline{d})$$

ce qui montre que f est injective.

ii) Montrons que f est surjective:

soit $y \in E/R \times F/S$

Il existe alors $u \in E/R$ et

$v \in F/S$ tels que

$$y = (u, v)$$

Il existe donc $a \in E$ et $b \in F$

tels que $u = \overline{a}$ et $v = \overline{b}$

$$\text{On a } f(\overline{a}, \overline{b}) = (\overline{a}, \overline{b})$$

$$f(\overline{a}, \overline{b}) = (u, v)$$

$$f(\overline{a}, \overline{b}) = y$$

ce qui montre que f est surjective et

par conséquent f est bijective.

Ex 4:

$$(a, b) R (c, d) \Leftrightarrow ad = bc$$

2. soit p et q deux éléments de $\mathbb{Z}$ premiers entre eux

$$(\overline{p}, \overline{q}) = \{ (pn, qn) / n \in \mathbb{Z}^* \}$$

On a:

$$(\overline{p}, \overline{q}) = \{ (x, y) \in E / (p, q) R (x, y) \}$$

$$= \{ (x, y) \in E / py = qx \}$$

Soit $(x, y) \in (\overline{p}, \overline{q})$ Alors on a

$$py = qx$$

On en déduit que p/qx

et comme $pq = 1$ on a p/x

Il existe donc $n \in \mathbb{Z}^*$ tel que $x = pn$.

De même on a

$$q/py \text{ et comme } pq = 1$$

$$\text{On a } q/y$$

Il existe donc $k \in \mathbb{Z}^*$ tq

$$y = qk$$

Ainsi l'égalité $py = qx$

$$\text{devient } pqk = pqn$$

Donc $k = n$ et par suite

$$(x, y) = (pn, nq)$$

Il en résulte que $(\overline{p}, \overline{q}) \subset \{ (pn, nq) / n \in \mathbb{Z}^* \}$



et comme $\{(np, nq) / n \in \mathbb{Z}^*\} \subset (\overline{p, q})$

on a donc

$$(\overline{p, q}) = \{(np, nq) / n \in \mathbb{Z}^*\}$$



SERIE 4

Exercice 1.4

On considère dans $\mathbb{R}[X]$ les deux polynômes :

$$A = 1 + 2X + \frac{7}{2}X^2 + \frac{26}{3}X^3 + \frac{173}{24}X^4 + \frac{27}{8}X^5 + \frac{13}{12}X^6 + \frac{1}{4}X^7 \quad B = 1 + X + \frac{1}{2}X^2 + \frac{1}{6}X^3 + \frac{1}{24}X^4$$

Montrer que B divise A dans $\mathbb{R}[X]$.

Exercice 2.4

On considère dans $\mathbb{R}[X]$ les deux polynômes :

$$A = 2 - X + 5X^2 - 7X^3 + 10X^4 - 14X^5 + 12X^6 - 9X^7 + 5X^8$$

$$B = 1 - X + 2X^2 - 3X^3 + 4X^4 - 5X^5$$

Effectuer la division euclidienne de A par B.



Exercice 3.4

Soit $A = 2X^8 - 2X^7 + 4X^6 + 2X^5 - 2X^4 + 10X^3 - 6X^2 + 6X - 2$

$$B = 2X^5 - 2X^4 + 4X^3 - 2X^2 + 2X$$

Déterminer $A \wedge B$ dans $\mathbb{R}[X]$.

Exercice 4.4

On considère dans $\mathbb{R}[X]$ l'élément : $P = 2X^2 - 4X^3 + X^4 + 3X^5 - 3X^6 + X^7$

1) Déterminer P' et P'' .

2) Déterminer les racines réelles de P.

3) Montrer que le polynôme $X^2 - 2X + 2$ est irréductible dans $\mathbb{R}[X]$.

4) Donner la décomposition de P en produit de facteurs irréductibles dans $\mathbb{R}[X]$.

Exercice 5.4

Soit m et n deux entiers naturels non nuls tels que $m > n$. Soit q le quotient et r le reste de la division euclidienne de m par n. On considère dans $\mathbb{R}[X]$ les deux éléments $A = X^m - 1$ et $B = X^n - 1$.

1) Calculer $(X^n - 1)(X^{nq+r-n} + X^{nq+r-2n} + \dots + X^r) + X^r - 1$.

2) Effectuer la division euclidienne de A par B.

3) Montrer que $A \wedge B = X^d - 1$ où $d = m \wedge n$.

Exercice 6.4

Soit $n \in \mathbb{N}^*$. Montrer que :

$$A = (X + 1)^{2n} - X^{2n} - 2X - 1 \text{ est divisible par } B = X(X + 1)(2X + 1) \text{ dans } \mathbb{R}[X].$$

Exercice 7.4

Trouver un élément unitaire P de degré ≤ 3 dans $\mathbb{R}[X]$ tel que le reste de la division euclidienne de P par $X+1$, $X-1$, $X+2$ soit égal à 3.

Serie 4 :

Polynômes <3>

Ex 1

$$A = 1 + 2x + \frac{1}{2}x^2 + \frac{26}{3}x^3 + \frac{173}{2}x^4 + \frac{27}{3}x^5 + \frac{13}{12}x^6 + \frac{1}{4}x^7$$

$$B = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4$$

Pe B divise A dans $\mathbb{R}[X]$

$$\frac{1}{7}x^7 + \frac{13}{12}x^6 + \frac{27}{8}x^5 + \frac{173}{24}x^4 + \frac{26}{3}x^3 + \frac{7}{2}x^2 + 2x + 1 \quad \left| \quad \frac{1}{24}x^4 + \frac{1}{6}x^3 + \frac{1}{2}x^2 + x + 1 \right.$$

$$\frac{1}{4}x^7 + x^6 + 3x^5 + 6x^4 + 6x^3$$

$$6x^3 + 2x^2 + x + 1$$

$$\frac{1}{12}x^6 + \frac{3}{8}x^5 + \frac{29}{24}x^4 + \frac{8}{3}x^3 + \frac{7}{2}x^2 + 2x + 1$$

$$\frac{1}{12}x^6 + \frac{1}{3}x^5 + x^4 + 2x^3 + 2x^2$$

$$\frac{1}{24}x^5 + \frac{5}{24}x^4 + \frac{2}{3}x^3 + \frac{3}{2}x^2 + 2x + 1$$

$$\frac{1}{24}x^5 + \frac{1}{6}x^4 + \frac{1}{2}x^3 + x^2 + x$$

$$\frac{1}{24}x^4 + \frac{1}{6}x^3 + \frac{1}{2}x^2 + x + 1$$

$$\frac{1}{2}x^4 + \frac{1}{6}x^3 + \frac{1}{2}x^2 + x + 1$$

0

Donc B divise A. $A = QB$

$$A = B (6x^3 + 2x^2 + x + 1)$$

Ex 2:

$$A = 2 - X + 5X^2 - 7X^3 + 10X^4 - 14X^5 + 12X^6 - 9X^7 + 5X^8$$

$$B = 1 - X + 2X^2 - 3X^3 + 4X^4 - 5X^5$$

Estimer la D.E. de A par B

$$5X^8 - 9X^7 + 12X^6 - 14X^5 + 10X^4 - 7X^3 + 5X^2 - X + 2 \quad - 5X^5 + 4X^4 - 3X^3 + 2X^2 - X + 1$$

$$- 5X^8 + 4X^7 - 3X^6 + 2X^5 - X^4 + X^3$$

$$- 5X^7 + 9X^6 - 12X^5 + 9X^4 - 6X^3 + 5X^2 - X + 2$$

$$- X^3 + X^2 - X + 1 = R$$

$$5X^7 - 4X^6 + 3X^5 - 2X^4 + X^3 - X^2$$

$$5X^6 - 9X^5 + 7X^4 - 5X^3 + 4X^2 - X + 2$$

$$- 5X^6 + 4X^5 - 3X^4 + 2X^3 - X^2 + X$$

$$- 5X^5 + 4X^4 - 3X^3 + 3X^2 + 2$$

$$5X^5 - 4X^4 + 3X^3 - 2X^2 + X - 1$$

$$X^2 + X + 1 = R$$

$$A = QB + R$$

$$A = B(-X^3 + X^2 - X + 1) + (X^2 + X + 1)$$

SMIA 2

Ex 3

$$\text{Soit } A = 2X^9 - 2X^7 + 4X^6 + 2X^5 - 2X^4 + 10X^3 - 6X^2 + 6X - 2$$

$$B = 2X^5 - 2X^4 + 4X^3 - 2X^2 + 2X$$

Déterminer $A \div B$ dans $\mathbb{R}[X]$. (On utilisera l'algorithme d'Euclide).

i) On effectue la DE de A par B.

$$\begin{array}{r|l} 2X^9 - 2X^7 + 4X^6 + 2X^5 - 2X^4 + 10X^3 - 6X^2 + 6X - 2 & 2X^5 - 2X^4 + 4X^3 - 2X^2 + 2X \\ - 2X^9 + 2X^7 - 4X^6 + 2X^5 - 2X^4 & \\ \hline & 4X^5 - 4X^4 + 10X^3 - 6X^2 + 6X - 2 \\ & - 4X^5 + 4X^4 - 8X^3 + 4X^2 - 4X \\ \hline & 2X^3 - 2X^2 + 2X - 2 \end{array} \quad \begin{array}{l} X^3 + 2 \end{array}$$

$$R_1 = 2X^3 - 2X^2 + 2X - 2$$

ii) On fait la DE de B par R_1 .

$$\begin{array}{r|l} 2X^5 - 2X^4 + 4X^3 - 2X^2 + 2X & 2X^3 - 2X^2 + 2X - 2 \\ - 2X^5 + 2X^4 - 4X^3 + 2X^2 & \\ \hline & 2X^3 + 2X \\ & - 2X^3 + 2X^2 + 2X - 2 \\ \hline & 2X^2 + 2 \end{array} \quad \begin{array}{l} X^2 + 1 \end{array}$$

$$R_2 = 2X^2 + 2$$

SMIA2

iii) On effectue la DE de R_1 par R_2 .

$2X^3 - 2X^2 + 2X - 2$	$2X^2 + 2$
$- 2X^2 + 2X$	
$- 2X^2 - 2$	$X - 1$
$- 2X^2 - 2$	
0	

SMIA2

$$R_3 = 0$$

iv) $A \wedge B = 2X^2 + 2 = X^2 + 1$

Pgcd est unitaire

$$\boxed{A \wedge B = X^2 + 1}$$

Ex 5:

$$n, r \in \mathbb{N}^+ \quad m > n$$

$$m = nq + r \quad \text{avec } 0 \leq r < n$$

$$A = X^m - 1$$

$$B = X^n - 1$$

$$1) C = (X^n - 1) (X^{nq+r-0} + X^{nq+r-2n} + \dots + X^r) + X^r - 1$$

on a

$$C = X^{nq+r} + X^{nq+r-n} + \dots + X^{nq+r-n} - X^{nq+r-n} - X^{nq+r-2n} - \dots - X^{nq+r-3n} - \dots - X^r + X^r - 1$$

$$C = X^{nq+r} - 1 = X^m - 1$$

$$2) \text{ On a } A = BQ + (X^r - 1)$$

$$\deg(X^r - 1) = r < n = \deg B$$

$$3) \text{ Montrer que } (X^m - 1) \wedge (X^n - 1) = X^d - 1$$

D'après 2) on a

$$(X^m - 1) \wedge (X^n - 1) = (X^n - 1) \wedge (X^r - 1)$$

on effectue la D.E de n par r.

On obtient

$$n = rq_1 + r_1 \quad (0 \leq r_1 < r)$$

D'après 2) on a

$$(X^n - 1) \wedge (X^r - 1) = (X^{r_1} - 1) \wedge (X^n - 1)$$

En effectuant la D.E de r par r_1,

$$(r = r_1 q_2 + r_2)$$

$$\text{On a } (X^r - 1) \wedge (X^{r_1} - 1) = (X^{r_2} - 1) \wedge (X^{r_1} - 1)$$

soit r_2 le dernier reste non nul

$$r_{t-2} = r_{t-1} q_t + r_t$$

$$r_{t-1} = r_t q_{t+1}$$

$$(X^{r_{t-2}} - 1) \wedge (X^{r_{t-1}} - 1) = (X^{r_{t-1}} - 1) \wedge (X^{r_t} - 1)$$

$$(X^{r_{t-1}} - 1) \wedge (X^{r_t} - 1) = (X^{r_t} - 1) \wedge (X^{r_{t+1}} - 1)$$

$$= (X^{r_t} - 1) \wedge 0$$

$$= X^{r_t} - 1$$

$$\text{Donc: } (X^m - 1) \wedge (X^n - 1) = X^{r_t} - 1$$



Autre méthode pour montrer que

$$(X^m - 1) \mid (X^n - 1) \iff X^d - 1 \text{ où } d = \text{m.p.p.}(m, n)$$

Cette méthode est basée sur le résultat

Tout polynôme $A \in \mathbb{C}[X]$ de degré ≥ 1

admet une racine dans $\mathbb{C}$ alors

$$z \text{ racine de } X^m - 1 \iff z^m = 1$$

$$z = e^{\frac{ik\pi}{m}}, \quad 0 \leq k \leq m-1$$

$$z \text{ racine de } X^m - 1 \iff \exists k \in \{0, 1, \dots, m-1\} \text{ tel que } z = e^{\frac{ik\pi}{m}}$$

$$U_m = \{z \in \mathbb{C} / z^m = 1\}$$

$$U_n = \{z \in \mathbb{C} / z^n = 1\}$$

$$\text{si } z \in U_m \cap U_n$$

Alors on a z est racine de $X^d - 1$

En effet posons $m = du$ et $n = dv$.

$$z = e^{\frac{ik\pi}{m}} \text{ et } z = e^{\frac{it\pi}{n}}$$

$$\Rightarrow e^{\frac{ik\pi}{m}} = e^{\frac{it\pi}{n}}$$

$$\Rightarrow \frac{2k\pi}{m} = \frac{2t\pi}{n}$$

$$\Rightarrow kn = mt$$

$$\Rightarrow kv = tu$$

$$\Rightarrow v/tu$$

$$\text{or } uv = 1$$

$$\Rightarrow v/t$$

$$\Rightarrow t = v\beta$$

$$k = u\alpha$$

$$\text{D'où } z = e^{\frac{ik\pi}{m}} = e^{\frac{2i\alpha\pi}{du}} = e^{\frac{2i\beta\pi}{dv}}$$

$$\Rightarrow \frac{2\alpha\pi}{du} = \frac{2\beta\pi}{dv}$$

$$\Rightarrow -\alpha = -\beta$$

$$z = e^{\frac{2ik\pi}{m}} = e^{\frac{2i\alpha\pi}{du}} = e^{\frac{2i\beta\pi}{dv}} \text{ avec}$$

$$0 \leq \alpha \leq d-1$$

Donc z est racine de $X^d - 1$.



$$D^0 f = B \in K[X]$$

$$B/A \in \exists Q \in K[X] / A = BQ$$

th: $B/A \Leftrightarrow$ le reste de la D.E. de A par B est nul.

Ex 6:

Soit $n \in \mathbb{N}^*$

Montrer que

$$A = (X+1)^{2n} - X^{2n} - 2X - 1$$

est divisible par $X(X+1)(2X+1)$

$$\text{on a } \tilde{A}(0) = (0+1)^{2n} - 0^{2n} - 2 \times 0 - 1$$

$$= 1 - 0 - 0 - 1$$

$$= 0$$

0 est donc racine de A dans $\mathbb{R}$

on en déduit que X/A

Il existe donc $Q_1 \in \mathbb{R}[X]$ tel que

$$A = XQ_1$$

$$\text{on a } \tilde{A}(-1) = 0$$

-1 est racine de A dans $\mathbb{R}$

$$\Rightarrow (X+1)/A \text{ dans } \mathbb{R}[X]$$

c'est à dire $(X+1)XQ_1$

comme X et $(X+1)$ sont premiers entre eux, on a $(X+1)/Q_1$

$$\text{et : } Q_1 = (X+1)Q_2 ; Q_2 \in \mathbb{R}[X].$$

aussi on a

$$A = X(X+1)Q_2$$

$$\text{On a } \tilde{A}\left(-\frac{1}{2}\right) = \left(\frac{1}{2}\right)^{2n} - \left(-\frac{1}{2}\right)^{2n} + 1 - 1 = 0$$

$-\frac{1}{2}$ est donc racine de A dans $\mathbb{R}$

$$\Rightarrow (X + \frac{1}{2})/A \text{ dans } \mathbb{R}[X].$$

$$\text{et } (X + \frac{1}{2})/X(X+1)Q_2$$

$$\text{comme } (X + \frac{1}{2}) \wedge X = 1$$

on a d'après Gauss

$$(X + \frac{1}{2})/(X+1)Q_2$$

$$\text{De même comme } (X + \frac{1}{2}) \wedge (X+1) = 1,$$

$$\text{on a } (X + \frac{1}{2})/Q_2$$

$$\Rightarrow Q_2 = (X + \frac{1}{2})Q_3$$

$$= (X + \frac{1}{2})^2 \left(\frac{1}{2}\right)Q_3$$

$$= (2X+1) \left(\frac{1}{2}\right)Q_3$$

$$A = X(X+1)(2X+1) \left(\frac{1}{2}Q_3\right)$$

$$\Rightarrow X(X+1)(2X+1)/A \text{ dans } \mathbb{R}[X].$$

Ex 7:

Trouver un $\tilde{P} \in \mathbb{R}[X]$ de degré ≤ 3

tel que le reste de la D.E. de P par

$X+1$, $X-1$ et $X+2$ soit 3.

$$P = (X+1)Q_1 + 3 \quad (1)$$

$$P = (X-1)Q_2 + 3 \quad (2)$$

$$P = (X+2)Q_3 + 3 \quad (3)$$

$$(1) - (2) \Rightarrow (X+1)Q_1 = (X-1)Q_2$$

$$\Rightarrow (X-1)/(X+1)Q_1$$

$$\text{comme } (X-1) \wedge (X+1) = 1$$

$$\text{on a } (X-1)/Q_1$$

$$\text{D'où } Q_1 = (X-1)Q_4$$

$$\text{et } P = (X+1)(X-1)Q_4 + 3 \quad (4)$$

$$(4) - (3) \Rightarrow$$

$$(X+1)(X-1)Q_4 = (X+2)Q_3$$

$$\Rightarrow X+2/Q_4$$

$$Q_4 = (X+2)Q_5$$

$$\text{Donc } P = (X+1)(X-1)(X+2)Q_5 + 3$$

$$\text{avec } \deg Q_5 = 0$$



SERIE 5

Exercice 1.5

Soit $(E, \top)$ et $(F, \perp)$ deux groupes.

On considère dans $E \times F$ la loi de composition interne $*$ définie par :

$$(u, v) * (x, y) = (u \top x, v \perp y)$$

1) Montrer que $(E \times F, *)$ est un groupe.

2) Soit H un sous-groupe de $(E, \top)$ et J un sous-groupe de $(F, \perp)$.

Montrer que $H \times J$ est un sous-groupe de $(E \times F, *)$.

Exercice 2.5

Soit H et J deux sous-groupes d'un groupe $(G, \top)$. On pose :

$$H \top J = \{x \top y / x \in H, y \in J\}.$$

Montrer que $H \top J$ est un sous-groupe de $(G, \top)$.

Exercice 3.5

Déterminer tous les sous-groupes du groupe symétrique S_3 .

Exercice 4.5

Soit $(G, \top)$ un groupe et H une partie finie de G stable pour $\top$.

Montrer que H est un sous-groupe de $(G, \top)$.

Exercice 5.5

Soit $(G, \top)$ un groupe tels que pour tout élément x de G on a : $x^{-1} = x$.

1) Montrer que $(G, \top)$ est abélien.

2) Si G est fini, montrer qu'il existe $n \in \mathbb{N}$ tel que : $0(G) = 2^n$.

Exercice 6.5

Soit $(G, \top)$ un groupe cyclique d'ordre n engendré par a .

1) Soit $k \in \{1, 2, \dots, n-1\}$ et $b = a^k$.

Montrer que b est générateur de $(G, \top)$ si et seulement si k est premier avec n .

2) On suppose $n = 12$. Déterminer tous les générateurs de $(G, \top)$.



Exercice 7.5

Soit p un nombre premier. On définit dans $G = \mathbb{Z}/p\mathbb{Z} - \{0\}$ une multiplication par :

$$\overline{x} \cdot \overline{y} = \overline{xy}.$$

1) Montrer que $(G, \cdot)$ est un groupe.

2) Montrer que pour tout élément x de $\mathbb{Z}$ on a : p divise $x^p - x$.

Exercice 8.5

Soit (G, T) un groupe abélien et H un sous-groupe de (G, T) tel que G/H soit fini d'ordre n .

Montrer que pour tout $x \in G$, on a : $x^n \in H$.

Exercice 9.5

Soit (E, T) un groupe cyclique d'ordre m engendré par a et $(F, \perp)$ un groupe cyclique d'ordre n engendré par b tels que m et n soient premiers entre eux.

Montrer que le groupe produit $E \times F$ est cyclique.

Exercice 10.5

Soit $(E, T); (F, *)$ deux groupes commutatifs finis d'ordre respectivement m, n tels que m et n soient premiers entre eux, e l'élément neutre de (E, T) , f l'élément neutre de $(F, *)$ et ϕ un homomorphisme de groupes de (E, T) dans $(F, *)$.

Soit a un élément de E d'ordre p , $b = \phi(a)$ et q l'ordre de b .

1) Montrer que q divise p .

2) Montrer que q divise m .

3) Montrer que $q = 1$.

4) Montrer que pour tout élément x de E on a $\phi(x) = f$.

Exercice 11.5

Soit (G, T) un groupe commutatif fini d'ordre $n = pq$ où p et q sont deux nombres premiers distincts.

1) On suppose dans cette question que tout élément de G distinct de l'élément neutre e est d'ordre p .

Soit g un élément de G distinct de e et soit H le sous-groupe de (G, T) engendré par g .

a) Déterminer $O(G/H)$.

b) Soit x un élément de G n'appartenant pas à H .

i) Déterminer $O(\bar{x})$ où $\bar{x}$ désigne la classe d'équivalence de x modulo H .

ii) Montrer que $x^q \in H$.

iii) Calculer $\bar{x}^q$.

iv) Montrer que q divise p .

v) Que peut-on conclure ?

2) Montrer qu'il existe un élément a de G d'ordre p et un élément b de G d'ordre q .

3) Soit $c = a T b$. Déterminer $O(c)$.

4) Montrer que G est cyclique.



Exercice (Hors série)

Soit E un ensemble, on considère dans $P(E)$ la loi de composition interne Δ

définie par :

$$X \Delta Y = (X - Y) \cup (Y - X)$$

Montrer que $(P(E), \Delta)$ est un groupe abélien.

$(P(E), \Delta)$, groupe abélien si

Δ associative

Δ est commutative

Δ admet un él^é neutre

Tout élément de $P(E)$ est inversible

solution :

i. Soit $x, y \in P(E)$, on a

$$\begin{aligned} x \Delta y &= (x - y) \cup (y - x) \\ &= (y - x) \cup (x - y) \\ &= y \Delta x \end{aligned}$$

Δ est donc commutative

ii. Soit x, y et z trois éléments de $P(E)$ on a

$$\begin{aligned} (x \Delta y) \Delta z &= (x - y) \cup (y - x) - z \\ &\quad \cup [z - (x - y) \cup (y - x)] \end{aligned}$$

$$\text{et } x \Delta (y \Delta z) = [x - (y - z) \cup (z - y)] \cup [(y - z) \cup (z - y) - x]$$

Soit $x \in (x \Delta y) \Delta z$ on a

$$x \in [(x - y) \cup (y - x)] - z$$

$$\text{ou } x \in z - [(x - y) \cup (y - x)]$$

$$a. \text{ si } x \in [(x - y) \cup (y - x)] - z$$

$$\text{on a } x \in (x - y) \cup (y - x) \text{ et } x \notin z$$

$$x \in x - y \text{ ou } x \in y - x \text{ et } x \notin z$$

$$\text{si } x \in x - y \text{ on a alors } x \in x$$

$$\text{et } x \notin y \text{ et } x \notin z$$

$$\Rightarrow x \notin y - z \text{ et } x \notin z - y$$

$$\Rightarrow x \notin (y - z) \cup (z - y)$$

$$\Rightarrow x \in x - [(y - z) \cup (z - y)]$$

$$\text{D'où } x \in x \Delta (y \Delta z)$$

$$\text{si } x \in y - x \text{ on a } x \in y, x \notin x \text{ et } x \notin z$$

$$\text{on a } x \in y - z \text{ et } x \notin x$$

$$\text{D'où } x \in (y - z) \text{ et } x \notin x$$

$$\Rightarrow x \in [(y - z) \cup (z - y)] - x$$

$$\text{Donc } x \in x \Delta (y \Delta z)$$

$$b. \text{ si } x \in z - [(x - y) \cup (y - x)]$$

$$\text{on a } x \in z \text{ et } x \notin (x - y) \cup (y - x)$$

$$x \in z \text{ et } (x \notin (x - y) \text{ et } x \notin (y - x))$$

$$x \in z \text{ et } (x \notin x \text{ ou } x \in y) \text{ et } (x \notin y \text{ ou } x \in x)$$

$$\text{si } x \notin x \text{ on a } x \in (z - x)$$

$$\text{mais si } x \notin x \text{ on a } x \notin y$$

$$\text{on aura } x \in (z - y) \text{ et } x \in (y - z) \cup (z - y)$$

$$\Rightarrow x \in x \Delta (y \Delta z)$$

$$\text{si } x \in y \text{ on a alors } x \in x$$

$$\text{D'où } x \notin y - z \text{ et } x \notin z - y$$

$$\text{D'où } x \in (y - z) \cup (z - y)$$

$$\Rightarrow x \in x - [(y - z) \cup (z - y)]$$

$$\Rightarrow x \in x \Delta (y \Delta z)$$

$$\text{ainsi on a } (x \Delta y) \Delta z \subset x \Delta (y \Delta z)$$

on montre de façon analogue

$$x \Delta (y \Delta z) \subset (x \Delta y) \Delta z$$

en condition on a

$$(x \Delta y) \Delta z = x \Delta (y \Delta z)$$

ce qui montre que Δ est associative

iii. Soit $x \in P(E)$ on a

$$x \Delta \emptyset = (x - \emptyset) \cup (\emptyset - x)$$

$$= X \cup \emptyset = X$$

D'où φ est l'élément neutre de $P(E)$ pour Δ

iv. soit $X \in P(E)$, on a

$$X \Delta X = (X - X) \cup (X - X) = \emptyset \cup \emptyset = \emptyset$$

X est donc inversible pour Δ

$$\text{et } X^{-1} = X$$

D'après i), ii) et iv)

$(P(E), \Delta)$ est un groupe commutatif.

Ex (2):

Soit (G, T) un groupe I et J deux sous groupes de (G, T) tels que:

$$H = I \cup J, \text{ soit un sous groupe de } (G, T)$$

Montrer que $I \subset J$ ou $J \subset I$

Solution:

Supposons que $I \not\subset J$ et montrons que $J \subset I$.

Soit $x \in J$:

Comme $I \not\subset J$, il existe $a \in I$ tel que $a \notin J$

On a $x, a \in H$ et comme H est un sous groupe

$$xTa \in H$$

$$\text{D'où } xTa \in I \text{ ou } xTa \in J$$

si $xTa \in J$, on aura:

$$xTa = b \text{ avec } b \in J$$

$$\Rightarrow x^{-1}T(xTa) = x^{-1}Tb$$

$$\Rightarrow a = x^{-1}Tb$$

Mais comme $x \in J$, $b \in J$ et J un sous groupe

$$\text{on a } x^{-1}Tb \in J \text{ d'où } a \in J$$

ce qui contredit le fait que $a \notin J$

$$\text{Donc } xTa \in I$$

$$\text{En posant } xTa = c \text{ avec } c \in I$$

$$\text{On obtient } x = cTa^{-1} \in I$$

$$\text{Donc } J \subset I$$

$$xTa = c \\ xT(aTa^{-1}) = (cTa^{-1})$$



Ex 1.5:

Soit (E, T) et (F, L) deux gpes:

on considère dans $E \times F$ la loi de composition interne définie par:

$$(u, v) * (x, y) = (uTx, vLy)$$

1) Montrer que $(E \times F, *)$ est un groupe.

2) Soit H un sype de (E, T) et J un sype de (F, L) $H \times J$ est un sype de $(E \times F, *)$

A. i Associativité de $*$

Soit $(u, v), (x, y)$ et (z, t)

trois éléments de $E \times F$

$$\begin{aligned} \text{on a } [(u, v) * (x, y)] * (z, t) &= (uTx, vLy) * (z, t) \\ &= ((uTx)Tz, (vLy)Lt) \\ &= (uT(xTz), vL(yLt)) \\ &= (u, v) * (xTz, yLt) \\ &= (u, v) * [(x, y) * (z, t)] \end{aligned}$$

ce qui montre que $*$ est associative

ii. Element neutre pour $*$

Soit e l'élément neutre de (E, T)

et f l'élément neutre de (F, L)

Soit $(x, y) \in E \times F$.

On a:

$$\begin{aligned} (x, y) * (e, f) &= (xTe, yLf) = (x, y) \\ \text{et } (e, f) * (x, y) &= (eTx, yLy) = (x, y) \end{aligned}$$

Donc (e, f) est neutre pour $*$

iii. Existence de l'inverse

Soit $(x, y) \in E \times F$

on a

$$(x, y) * (x^{-1}, y^{-1}) = (xTx^{-1}, yLy^{-1}) = (e, f)$$

$$\text{et } (x^{-1}, y^{-1}) * (x, y) = (x^{-1}Tx, y^{-1}Ly) = (e, f)$$

Donc (x, y) est inversible pour $*$ et

$$(x, y)^{-1} = (x^{-1}, y^{-1})$$

Ex 2.5

Soit H et J deux sypes d'un gpe

com (G, T) on pose

$$HTJ = \{xTy / x \in H \text{ et } y \in J\}$$

Montrer que HTJ est un sype de (G, T)

i. Comme H et J sont des sypes de (G, T)

on a $e \in H$ et $e \in J$

D'où

$$e = eTe \in HTJ$$

et $HTJ \neq \emptyset$

ii) Soit x et y deux éléments de HTJ

Par définition de HTJ , il existe $a, c \in H$ et

$b, d \in J$ tels que

$$x = aTb \text{ et } y = cTd$$

$$\text{D'où } xTy^{-1} = (aTb)T(cTd)^{-1}$$

$$= (aTb)T(d^{-1}Tc^{-1})$$

$$= (aTb)T(c^{-1}Td^{-1})$$

$$= aT(bTc^{-1})Td^{-1}$$

$$= aT(c^{-1}Tb)Td^{-1}$$

$$= \underset{\substack{\uparrow \\ H}}{aTc^{-1}} \underset{\substack{\uparrow \\ J}}{bTd^{-1}}$$

$$xTy^{-1} = uTv$$

$$\text{avec } u = aTc^{-1} \in H$$

$$\text{et } v = bTd^{-1} \in J$$

$$\text{Donc } xTy^{-1} \in HTJ$$



Ex 1.5 suite

2i. Comme H est un sous-groupe de (G, T)

on a $e \in H$

De même comme J est un sous-groupe de (F, I)

on a $f \in J$, On en déduit que $(e, f) \in H \times J$

et par suite $H \times J \neq \emptyset$

ii. Soit (u, v) et (x, y) deux éléments de $H \times J$

on a :

$$(u, v) * (x, y)^{-1} = (u, v) * (x^{-1}, y^{-1}) \\ = (uTx^{-1}, vTy^{-1})$$

or: $uTx^{-1} \in H$ et $vTy^{-1} \in J$

D'où: $(uTx^{-1}, vTy^{-1}) \in H \times J$

Ex 3.5:

Déterminer tous les sous-groupes de $(S_3, \circ)$

On a $S_3 = \{e, \tau_{12}, \tau_{13}, \tau_{23}, f, g\}$

où

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{et} \quad g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Remarque:

Soit (G, T) un gpe

si G est fini ayant

n éléments alors tout sous-groupe H de (G, T)

est fini ayant un nombre d'éléments q

tel que $q \mid n$

i. sous-gp à un seul el $H_1 = \{e\}$

ii. sous-groupes à 6 éléments S_3

iii. Sous-gp à 2 éléments

$$H_2 = \{e, \tau_{12}\}$$

$$H_3 = \{e, \tau_{13}\}$$

$$H_4 = \{e, \tau_{23}\}$$

$$H_5 = \{e, g\}$$

iv. sous-groupes à 3 éléments.

$$H_6 = \{e, f, g\}$$

Ex 4.5

Soit (G, T) un groupe et H une partie finie non vide de G stable pour T

Montrer que H est un sous-groupe de (G, T)

Pour montrer que H est un sous-groupe il suffit de montrer que pour tout

$a \in H$, on a $a^{-1} \in H$.

soit $a \in H$:

$$f: H \rightarrow H$$

$$h \rightarrow aTh.$$

f est une injective

On en déduit que:

$$f(H) = H \text{ car } \text{card}(f(H)) = \text{card } H$$

puisque f est injective, il en résulte que

f est surjective, comme $a \in H$ il existe

alors $h \in H$ tel que $f(h) = a$

c'est à dire $aTh = a$

$$\Rightarrow h = e$$

$$\Rightarrow e \in H$$

comme $e \in H$ f est surjective, il existe un élément k de H tq $f(k) = e$.

c'est à dire : $aTb = e$

$$\Rightarrow b = a^{-1}$$

$$\Rightarrow a^{-1} \in H$$

$$H = \{h_1, h_2, \dots, h_n\}$$

$$aTh_1, aTh_2, \dots$$

Ex 5:

soit (G, T) un groupe abélien tel que

$$\forall x \in G : x^{-1} = x.$$

① $Mq(G, T)$ est abélien :

soit x et y deux éléments de G on a

$$xTy = x^{-1}Ty^{-1} = (yTx)^{-1} = yTx.$$

$xTy = yTx \Rightarrow$ Donc le groupe est commutatif.

② si G est fini, Mqu'il existe $n \in \mathbb{N}$

$$\text{tq } o(G) = 2^n$$

$$\text{si } o(G) = 1$$

$$\text{alors on a } o(G) = 2^0$$

$$\text{supposons } o(G) \geq 2$$

$$\text{soit } a \in G \text{ tq } a \neq e$$

$$H = \langle a \rangle = \{e, a\}$$

$$\text{on a } o(G/H) = \frac{o(G)}{o(H)} = \frac{o(G)}{2}$$

$$\Rightarrow o(G/H) < o(G)$$

on raisonne par récurrence sur $o(G)$

i. La propriété est vraie pour $o(G) = 1$.

ii. Hypothèse de récurrence, on suppose

la propriété vraie pour tout

$$k < o(G) = n$$

$$\text{Posons } o(G/H) = p$$

comme $p < o(G)$, on a d'après l'hypothèse de récurrence

$$o(G/H) = p = 2^t$$

$$\text{on } o(G) = o(H) o(G/H) = 2^{t+1}$$

SMIA2

Ex 8.5:

Soit (G, T) un gpe abélien et H un sype comme $m \wedge n = 1$ on a $q = 1$.

de (G, T) et que G/H sont fini d'ordre n

M.q $\forall x \in G \quad x^n \in H$

soit $x \in G$. $\bar{x}$ la classe d'équivalence de x modulo H

$\bar{x} \in G/H$

comme G/H est fini d'ordre n

$$\text{on a } \bar{x}^n = \bar{e}$$

$$\bar{x}^n = \bar{e}$$

$$\Rightarrow x^n \in H$$

Ex 10.5:

soit (E, T) et $(F, +)$ deux gpes com finis

$$o(E) = m, o(F) = n$$

$$m \wedge n = 1.$$

$$\varphi: E \rightarrow F$$

hom de gpes

$$a \in E \quad o(a) = p$$

$$b = \varphi(a) \quad o(b) = q$$

1) Montrer que q/p

2) Montrer que q/m

3) Montrer que $q=1$.

$$4) \forall x \in E, \varphi(x) = f.$$

solution:

$$1) \quad b^p = \varphi(a)^p = \varphi(a^p) = \varphi(e) = f.$$

D'où q/p .

2) On a d'après Lagrange

$$p/m$$

et d'après 1) on a q/p

$$\Rightarrow q/m$$

$$3) \text{ on a } q/m \text{ et } q/n$$

$$\text{comme } m \wedge n = 1 \text{ on a } q = 1.$$

$$4) \text{ soit } x \in E$$

$$\text{D'après 3) on a } o\varphi(x) = 1$$

$$\text{On en déduit que } \varphi(x) = f.$$

$$\varphi(\mathbb{Z}/\mathbb{Z}, +) \quad \bar{\varphi} \quad \varphi(\bar{1}) = \bar{e}$$

Ex 9:

(E, T) et $(F, +)$ deux gpes cycliques

$$E = \langle a \rangle$$

$$F = \langle b \rangle$$

$$o(E) = m$$

$$o(F) = n$$

$$m \wedge n = 1.$$

M.q $E \times F$ cyclique.

Ex 11.5:

(G, T) groupe com fini $o(G) = pq$.

p et q premiers, $p \neq q$

$$1) \forall x \in G, x \neq e \quad o(x) = p$$

soit $g \in G, g \neq e$.

$$H = \langle g \rangle$$

$$a. \quad o(G/H) = ?$$

$$b. \quad \text{soit } x \in G \setminus H$$

$$i. \quad o(\bar{x})$$

$$ii. \quad x^p \in H$$

$$iii. \quad x^{-p} = ?$$

$$iv. \quad q/p?$$

v. que peut on conclure?

solution:

i. a. on a d'après le th de Lagrange

$$o(G/H) = \frac{o(G)}{o(H)} = \frac{pq}{p} = q$$

b. i. comme $o(G/H) = q$, on a d'après

lagrange, $o(\bar{n})/q$, comme p est premier

on a $e(\bar{n}) = 1$ ou $e(\bar{n}) = q$,

mais comme $x \notin H$ on a $\bar{n} \neq \bar{e}$ et par suite

$$e(\bar{n}) = q$$

ii - comme $Q(\bar{x}) = q$

$$\text{on a } x^{-q} = \bar{e}$$

$$\text{or } x^{-q} = \overline{x^q}$$

$$\overline{x^q} = \bar{e}$$

Donc $x^q \in H$

iii - comme $x \neq e$ ($x \notin H$), on a d'après l'hypothèse

$$o(x) = p$$

$$\text{D'où } x^p = e \text{ et } \overline{x^p} = \bar{e}$$

$$\text{or } \overline{x^p} = \bar{x}$$

$$\text{D'où } \bar{x} = \bar{e}$$

iv - comme $e(\bar{x}) = q$ et $\bar{x} = \bar{e}$

$$\text{on a } q/p$$

v - D'après (iv) on a q/p comme p est premier

$$\text{on a } q = 1 \text{ ou } q = p \text{ Contradiction}$$

Il existe donc au moins un élément de G distinct

de e qui est d'ordre $\neq p$.

2) H qu'il existe $a, b \in G$ $o(a) = p$ et $o(b) = q$

D'après (1) il existe un élément $g \in G$, $g \neq e$

tel que: $o(g) \neq p$

$$\text{on a alors } o(g) = q \text{ ou } o(g) = n = pq$$

$$\text{si } o(g) = n = pq \text{ alors } \langle g \rangle = G$$

$$G = \{e, g, g^2, \dots, g^{n-1}\}$$

1^{er} cas:

$$\text{Soit } a = g^q$$

$$\text{on a } a \neq e$$

$$\text{et } a^p = (g^q)^p = g^{pq} = g^n = e$$

$$\Rightarrow o(a)/p$$

$$\Rightarrow o(a) = p$$

$$\text{soit } b = g^p$$

$$\Rightarrow o(b) = q$$

2^{ème} cas:

$$\text{si } o(g) = q$$

D'après D il existe un élément n de G ,

$n \neq e$ tel que $o(n) \neq q$

$$\text{on a } e(n) = p \text{ ou } o(n) = n = pq$$

$$\text{si } o(n) = p$$

$$\text{On prend } g = n \text{ et } b = g$$

$$\text{si } o(n) = n \text{ alors d'après le}$$

$$\text{premier cas } \langle n \rangle = G$$

$$\text{On prend } a = x^q \text{ et } b = x^p$$

3 - soit $C = aTb$ Déterminer $o(C)$

$$\text{Posons : } t = o(C)$$

$$t = 1 \text{ ou } t = p \text{ ou } t = n$$

$$\text{si } t = 1$$

$$\text{Alors : } aTb = e$$

$$\Leftrightarrow a = b^{-1}$$

$$b^{-1} \in \langle a \rangle \text{ et } b^{-1} \in \langle b \rangle$$

$$o(b^{-1})/p \text{ et } o(b^{-1})/q$$

$$\Rightarrow o(b^{-1}) = 1$$

$$\Rightarrow b = e \text{ contradiction}$$

$$\text{Donc } t \neq 1$$

$$\text{si } t = p$$

$$\text{on a } C^p = e$$

$$\text{càd } (aTb)^p = e$$

$$\text{or } a^p T b^p = e$$

$$\text{or } b^p = e \text{ contradiction}$$

$$\text{Donc } t \neq p$$

Demons $E \neq q$

Donc $t = n = pq$

$o(c) = n$

Montrer que G est cyclique:

comme $o(c) = n = pq = o(G)$

on a $\langle c \rangle = G$ ce qui montre que G est cyclique.

